

REMARKS

Claims 1-4, 20-22, 39-41 and 43 are pending in the application

In the Office Action, claims 1-4, 39-41 and 43 are rejected under 35 U.S.C. §101. In response, the claims have been amended to recite physical interaction with “multiple network data ports to connect to the network to receive and route requests to servers in the network.” This amendment is supported, for example, by page 9, line 12. Applicant respectfully submits that this amendment overcome the rejection under 35 U.S.C. §101.

In the Office Action, claims 1-4, 20-22 and 40-41 are rejected under 35 U.S.C. 103 over Menditto in view of Sadot; claim 39 is rejected under 35 U.S.C. 103 over Menditto in view of Sadot and Datar; and claim 43 is rejected under 35 U.S.C. 103 over Menditto in view of Sadot and Yang.

The claims have been amended to more clearly emphasize certain patentable distinctions over this art. Claim 1, which is representative, has been amended to recite the following limitation:

“, wherein the first persistence policy, if applicable, directs the service request to a server, currently or previously connected to the client, that is identified based on content of the service request, the content comprising server, session or cookie information within the service request at one or more layers corresponding to OSI layers 5-7, and wherein the second persistence policy, if applicable, directs the service request to a server, currently or previously connected to the client, that is identified based on client information within the service request or corresponding packet;”

This amendment clarifies (1) that “content” for purposes of claim 1 means “server, session or cookie information within the service request or corresponding packet at one or more layers corresponding to OSI layers 5-7,” (2) that the “first persistence policy” is a policy that, if applicable, “directs the service request to a server, currently or previously connected to the client, that is identified based on [the] content of the resource request,” and (3) that the “second persistence policy” is a policy that, if applicable, “directs the service request to a server, currently or previously connected to the client, that is identified based on client information within the service request or corresponding packet.” These amendments are supported, for example, by

page 16, lines 14-21, page 17, lines 1-2, 6-8, page 20, lines 18-19, page 21, lines 14-15, page 26, lines 3-11, page 28, lines 7-8, page 30, lines 2-3, 6-7, 21-22, 24-25.

In addition, the terms “content-aware” and “non-content aware” have been changed to “content-enabled” and “non-content-enabled.” These changes are supported, for example, by page 12, lines 19-22.

Thus, as amended, claim 1 requires first logic that is shared by and supports service requests for content-enabled and non-content-enabled services. When a service request from a client for content-enabled services is received, the first logic attempts to apply the first persistence policy and, if that is inapplicable, then attempts to apply the second persistence policy. When a service request for non-content-enabled services is received, the first logic attempts to apply the second persistence policy. The first persistence policy, if applicable, directs the service request to a server, currently or previously connected to the client, that is identified based on “content” of the service request, *i.e.*, server, session or cookie information within the service request or corresponding packet at one or more layers corresponding to OSI layers 5-7. The second persistence policy, if applicable, directs the service request to a server, currently or previously connected to the client, which is identified based on client information within the service request or corresponding packet. If neither of the persistence policies are applicable, second logic allocates a resource to the service request by applying a load balancing policy.

In the Office Action, the Examiner considers that Menditto meets the claim limitations regarding the “first logic,” “content-aware” and “non-content-aware” service requests, the “first persistence policy,” and the “second persistence policy.” (*See* Office Action, pages 3-4).

However, particularly in light of the foregoing amendments, it cannot be said that Menditto meets these claim limitations. The “content aware” request referred to at Col. 6, line 60, of Menditto is processed using a “classification” and/or “processing” policy, Col. 6, line 43, neither of which qualifies as the “first persistence policy.” To the contrary, the “classification” and/or “processing” policy of Menditto simply determines if the request qualifies for content processing based on the domain name, and, if so, routes the request to an appropriate content gateway processor 30. (*See* Col. 6, lines 61-67). There, the request is further parsed into its constituent parts, *e.g.*, application (http), domain name (www.honda.com), and object (images.accord.jpeg), which are then matched to entries in a content gateway directory 32. (*See*

Col. 6, lines 61-66). If a match is found, the request is deemed “classified,” and a connection is established to a server identified by the content gateway directory 32. (See Col.7, lines 1-5).

Significantly, through application of this “classification” and/or “processing” policy, there is no attempt to identify a server currently or previously connected to the client that originated the request. Rather, the “classification” and/or “processing” policy merely attempts to allocate a server to a request based on a classification of the request, which is insufficient. Nor is there any attempt to do so based on “content” of the request, *i.e.*, server, session or cookie information within the request or corresponding packet at one or more layers corresponding to OSI layers 5-7. Thus, because both of these requirements are expressly recited in claim 1 as amended, and the “classification” and/or “processing” policy of Menditto satisfies neither, it does not meet the claimed “first persistence policy.”

Nor does Menditto meet the claimed “second persistence policy.” There are three requirements of the “second persistence policy” expressed in claim 1 as amended: (1) that it attempts to identify a server currently or previously connected to the client originating the request; (2) that it do so based on client information within the request or corresponding packet; and (3) that it be potentially applicable to a request for content-enabled service if the first persistence policy is determined to be inapplicable.

The Office Action cites to Col. 6, lines 53-60, and Col. 10, lines 42-45, and claims these passages meet the claimed “second persistence policy,” but they do not. There are actually two procedures referred to in these passages. In the first, non-subscription traffic, which is apparently identified based on the domain name, is routed by the content gateway router 28, bypassing the content gateway processor 30. (See Col. 6, lines 56-60). This procedure does not qualify as the claimed “second persistence policy” because it (1) does not attempt to identify a server currently or previously connected to the client originating the request, (2) does not attempt to do so based on client information within the request or corresponding packet, (3) is not potentially applicable to a request for content-enabled service. Regarding requirement (1), merely identifying a server based on domain name and other attributes such as object does not necessarily identify a server currently or previously connected to the client that originated the request. Regarding requirement (3), note that any content aware request that is “qualified” is subscription traffic that is routed to

the content gateway processor 30 for processing, rendering the procedure for non-subscription traffic inapplicable to such requests. (*See* Col. 6, lines 60-67).

In the second procedure, content aware requests that cannot be classified because they do not have a matching classification in content gateway processor 30 lack a policy for request acceleration. (*See* Col. 10, lines 42-45). In this case, a domain name server proxy 38, through a query to domain name server 24, identifies a server based on the domain name. (*See* Col. 10:45-47). This procedure of identifying a server based on domain name does not qualify as the claimed “second persistence policy” because it (1) does not attempt to identify a server currently or previously connected to the client originating the request, and (2) does not attempt to do so based on client information within the request or corresponding packet. Regarding requirement (1), merely identifying a server based on domain name does not necessarily identify a server currently or previously connected to the client that originated the request.

In sum, Menditto fails to teach or suggest the claimed “first persistence policy” and the claimed “second persistence policy.” As established in the Dec. 19, 2007 Response to the previous Office Action, neither Sadot, Datar, nor Yang fill these gaps in teaching of Menditto. Therefore, the claims, as amended, patentably distinguish over these references, considered singly or in combination.

For all the foregoing reasons, reconsideration of and withdrawal of all outstanding rejections is respectfully requested. The Examiner is earnestly solicited to allow all claims, and pass this application to issuance.

To expedite allowance of this case, the Examiner is earnestly invited to call Robert C. Laurensen at (949) 759-5269.

Respectfully submitted,

Date: July 6, 2008

/Robert C. Laurensen/

Robert C. Laurensen

Reg No. 34,206

HOWREY LLP
2941 Fairview Park Drive, Box 7
Falls Church, VA 22042
FAX No. (703) 336-6950
Telephone No. (949) 759-5269